<Damn Vulnerable Shopping Cart>

<Group 1>

Product owner <Dr. Sreekumar>

<Amrita school of Engineering, Kollam >

Ashutosh A, Rakesh B, Mohit H
Raghuram K, Tarunkant G, Dhruv P

1 INTRODUCTION

“The world cant operate without software. Industries are controlled by software systems, as the financial systems, scientific labs, infrastructures and utilities, games, film, television, and the list goes on.”

Software engineering is an engineering discipline thats applied to the development of software in a systematic approach. Its the application of theories, methods, and tools to design build a software that meets the specifications efficiently, cost-effectively, and ensuring quality. Its not only concerned with the technical process of building a software, it also includes activities to manage the project, develop tools, testing, methods and theories that support the software production.

There are several existing methodologies to approach software building. Numerous models have been proposed till date with their respective pros and cons. No model is perfect and applicable to all softwares. Choice is made by the developer depending on the objective, constraints and resources available.

2 OBJECTIVE

Cybercrime is a global problem thats been dominating the news cycle. It poses a threat to individual security and an even bigger threat to large international companies, banks, and governments. Todays organized cybercrimes far out shadow lone hackers of the past now large organized crime rings function like start-ups and often employ highly-trained developers who are constantly innovating online attacks.

We have implemented an educational tool for our budding cyber security enthusiasts by which we can kick start their career in this field. A shopping cart has been designed in which we have deliberately injected vulnerabilities which can be exploited by a hacker, as to demonstrate the need of network security.

3 METHODOLOGY

Throughout the project we have followed **AGILE METHODOLOGY**. AGILE methodology is a practice that promotes continuous iteration of development and testing throughout the software development life cycle of the project.

3.1 PRINCIPLES OF AGILE

The following are the principles of AGILE methodology -

∗ Customer satisfaction by early and continuous delivery of valuable software.

∗ Face-to-face conversation is the best form of communication.

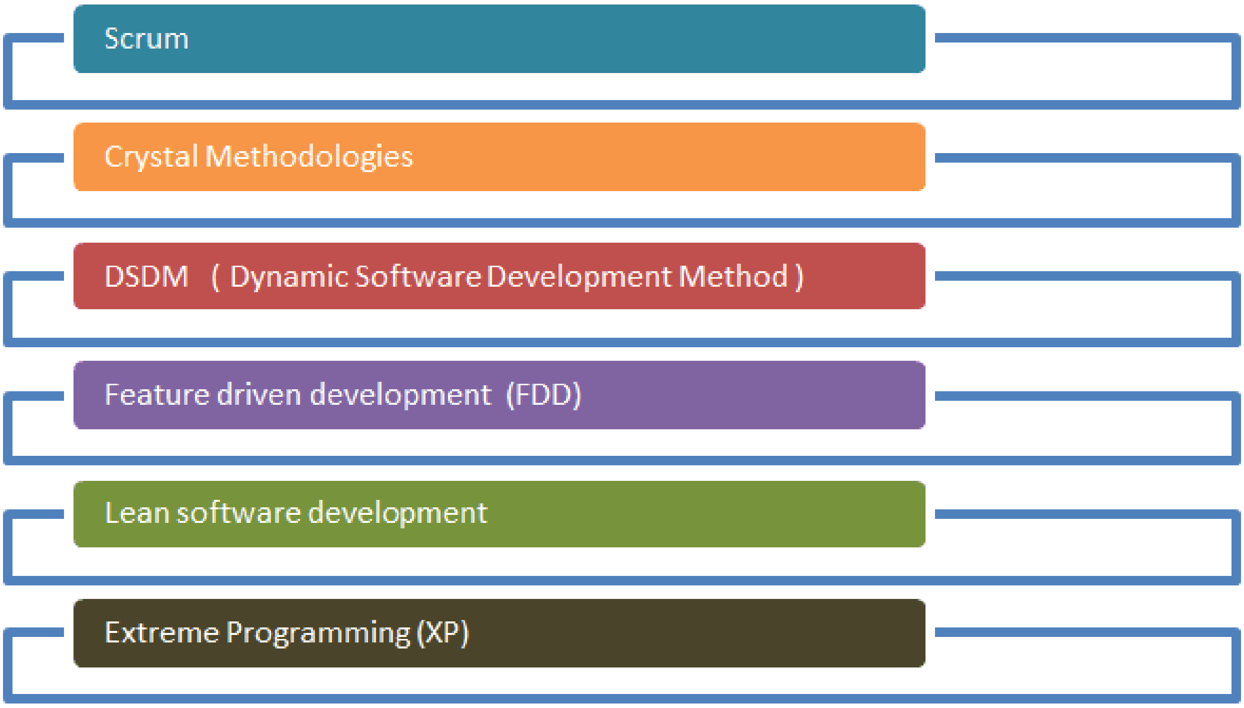
∗ KISS- Keep it simple !

∗ Best architectures, requirements, and designs emerge from self-organizing teams.

∗ Regularly, the team reflects on how to become more effective, and adjusts accordingly.

∗ Deliver working software frequently (weeks rather than months)

3.2 AGILE FRAMEWORKS



Scrum

Crystal Methodologies

DSDM (Dynamic Software Development Method)

Feature driven development (FDD)

Lean software development

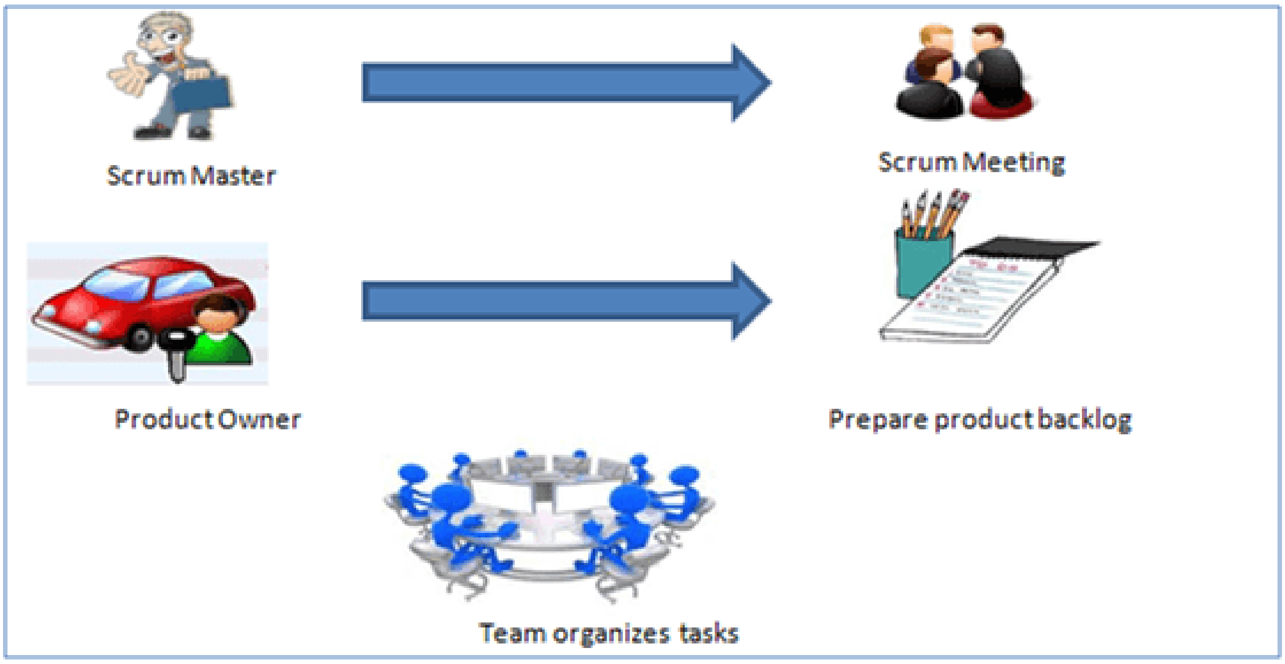
Extreme Programming (XP)

We have extensively followed **SCRUM Methodology** in our project. SCRUM is an agile development method which concentrates specifically on how to manage tasks within a team-based development environment.

It consists of three roles, and their responsibilities are explained as follows -

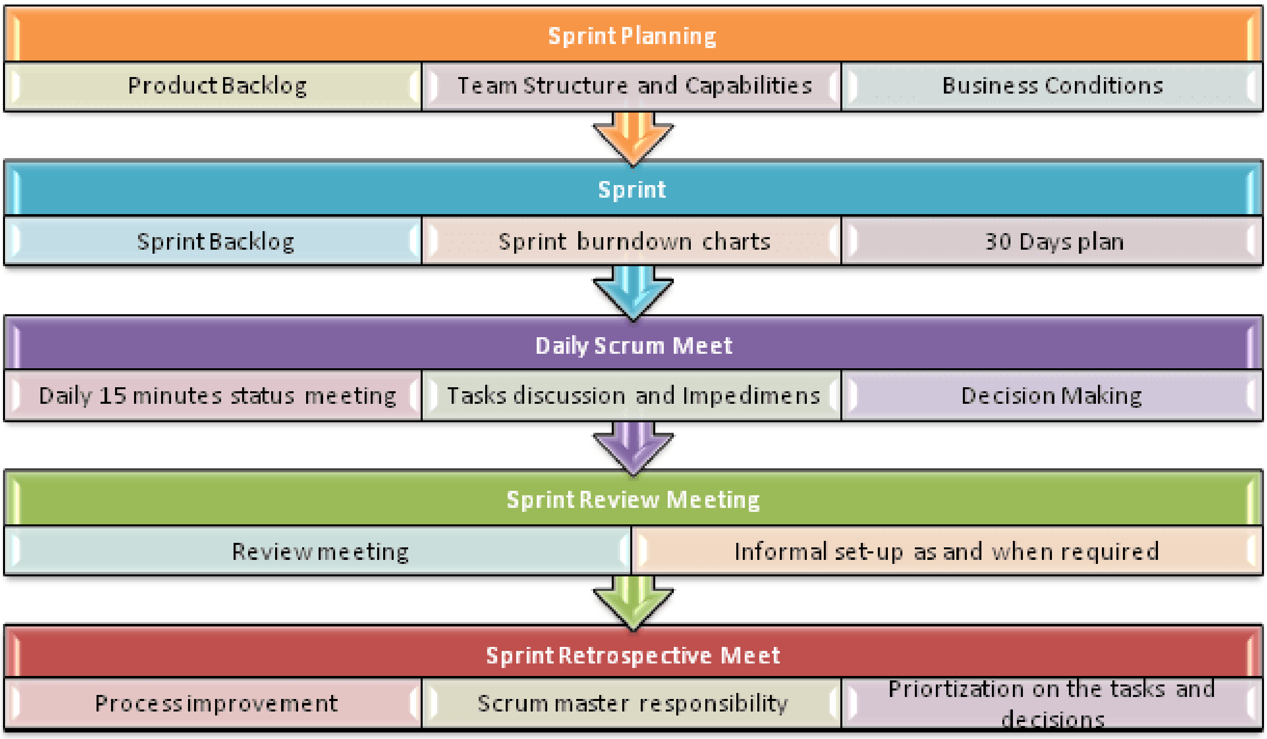
- **SCRUM MASTER** Master is responsible for setting up the team, sprint meeting and removes obstacles to progress.

- **PRODUCT OWNER** The Product Owner creates product backlog, prioritizes the backlog and is responsible for the delivery of the functionality at each iteration.
- **SCRUM TEAM** Team manages its own work and organizes the work to complete the sprint or cycle.



3.3 SCRUM PRACTICES

- Each iteration of a scrum is known as Sprint.
- Product backlog is a list where all details are entered to get end product.
- During each Sprint, top items of Product backlog are selected and turned into Sprint backlog.
- Team works on the defined sprint backlog.
- Team checks for the daily work.
- At the end of the sprint, team delivers product functionality.


Sprint Planning
Product Backlog
Team Structure and Capabilities
Business Conditions
Sprint
Sprint Backlog
Sprint burndown charts
30 Days plan
Daily Scrum Meet
Daily 15 minutes status meeting
Tasks discussion and Impedimens
Decision Making
Sprint Review Meeting
Review meeting
Informal set-up as and when required
Sprint Retrospective Meet
Process improvement
Scrum master responsibility
Priortization on the tasks and decisions

4 IMPLEMENTATION

We have done the implementation in following steps-

- **REQUIREMENT GATHERING** Understanding the need of customer is the main feature of AGILE modelling.
- **REQUIREMENT ANALYSIS** Analyzing the requirement gathered in order to obtain use full information.
- **CODING** Code the program as per the requirements modelled.
- **TESTING** Derive useful test cases in order to test the product.
- **EXECUTION** Deploy the product.

4.1 REQUIREMENT ENGINEERING

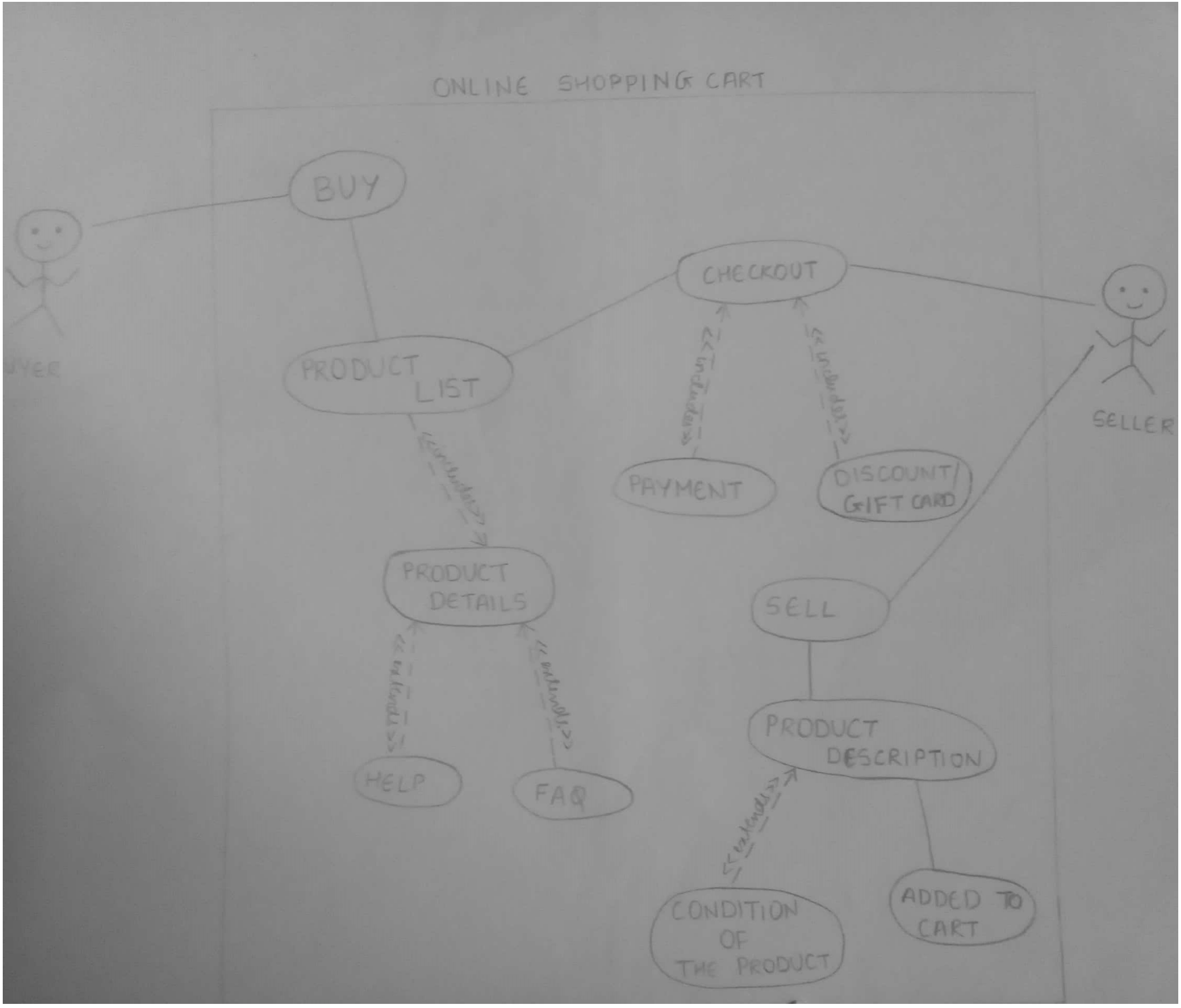
UML is an acronym that stands for Unified Modeling Language. Simply put, UML is a modern approach to modeling and documenting software.

The two most broad categories that encompass all other types are Behavioral UML diagram and

Structural UML diagram. As the name suggests, some UML diagrams try to analyze and depict the structure of a system or process, whereas other describe the behavior of the system, its actors, and its building components.

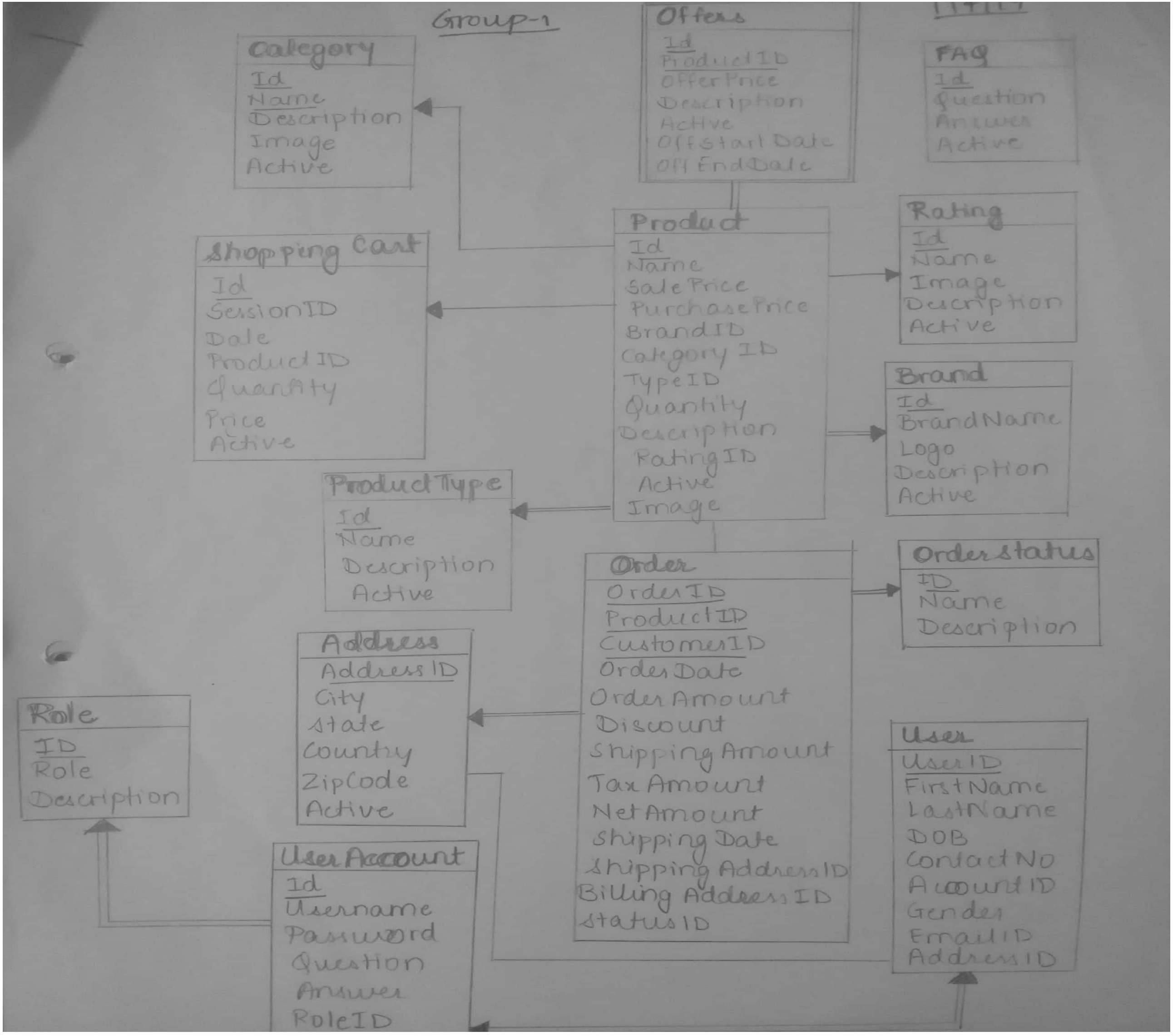
4.1.1 USE CASE DIAGRAM

Use case diagrams are valuable for visualizing the functional requirements of a system that will translate into design choices and development priorities.They also help identify any internal or external factors that may influence the system and should be taken into consideration.
They provide a good high level analysis from outside the system. Use case diagrams specify how the system interacts with actors without worrying about the details of how that functionality is implemented.



4.1.2 CLASS DIAGRAM

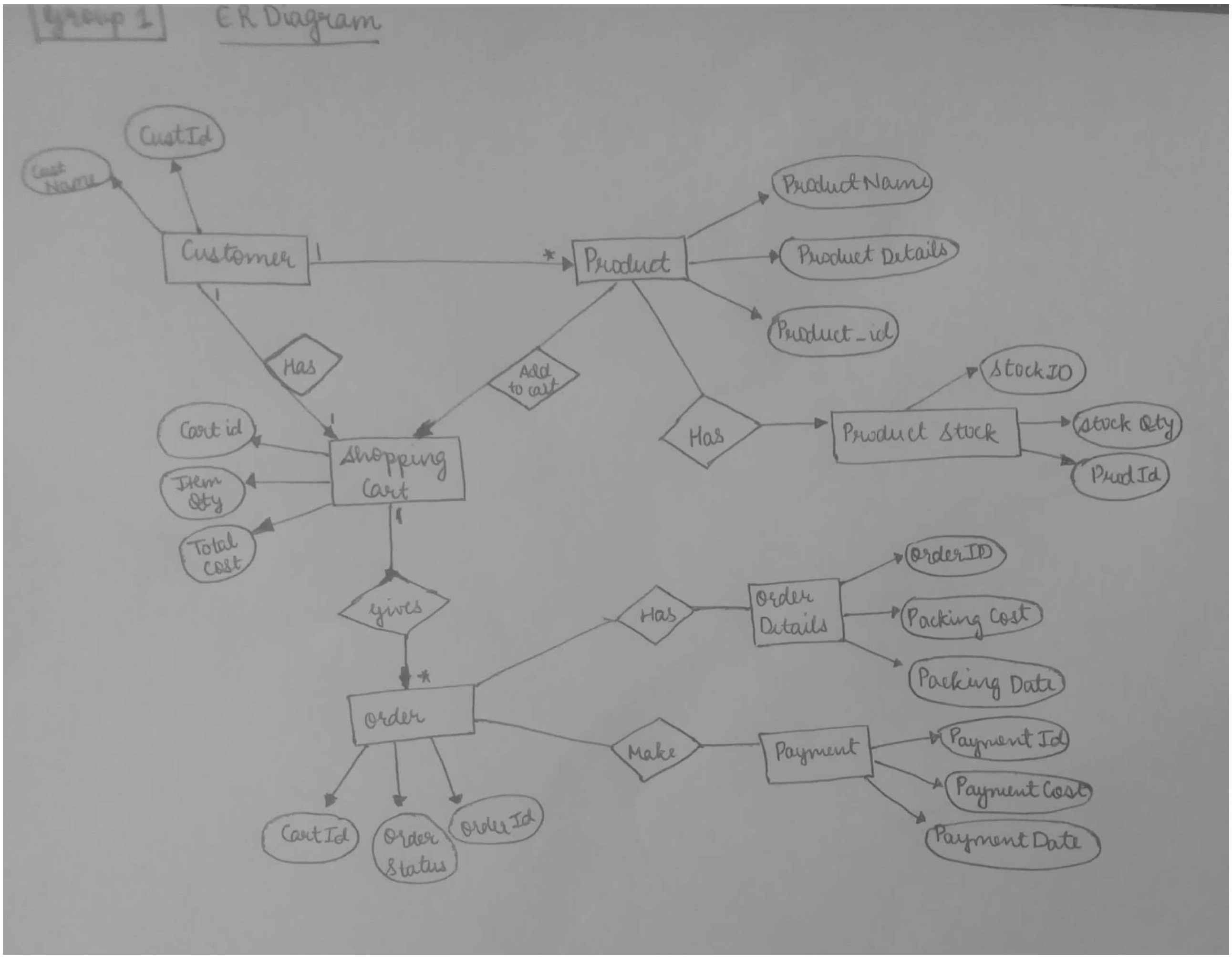
Class diagram is the most common diagram type for software documentation. Since most software being created nowadays is still based on the Object-Oriented Programming paradigm, using class diagrams to document the software turns out to be a common-sense solution.



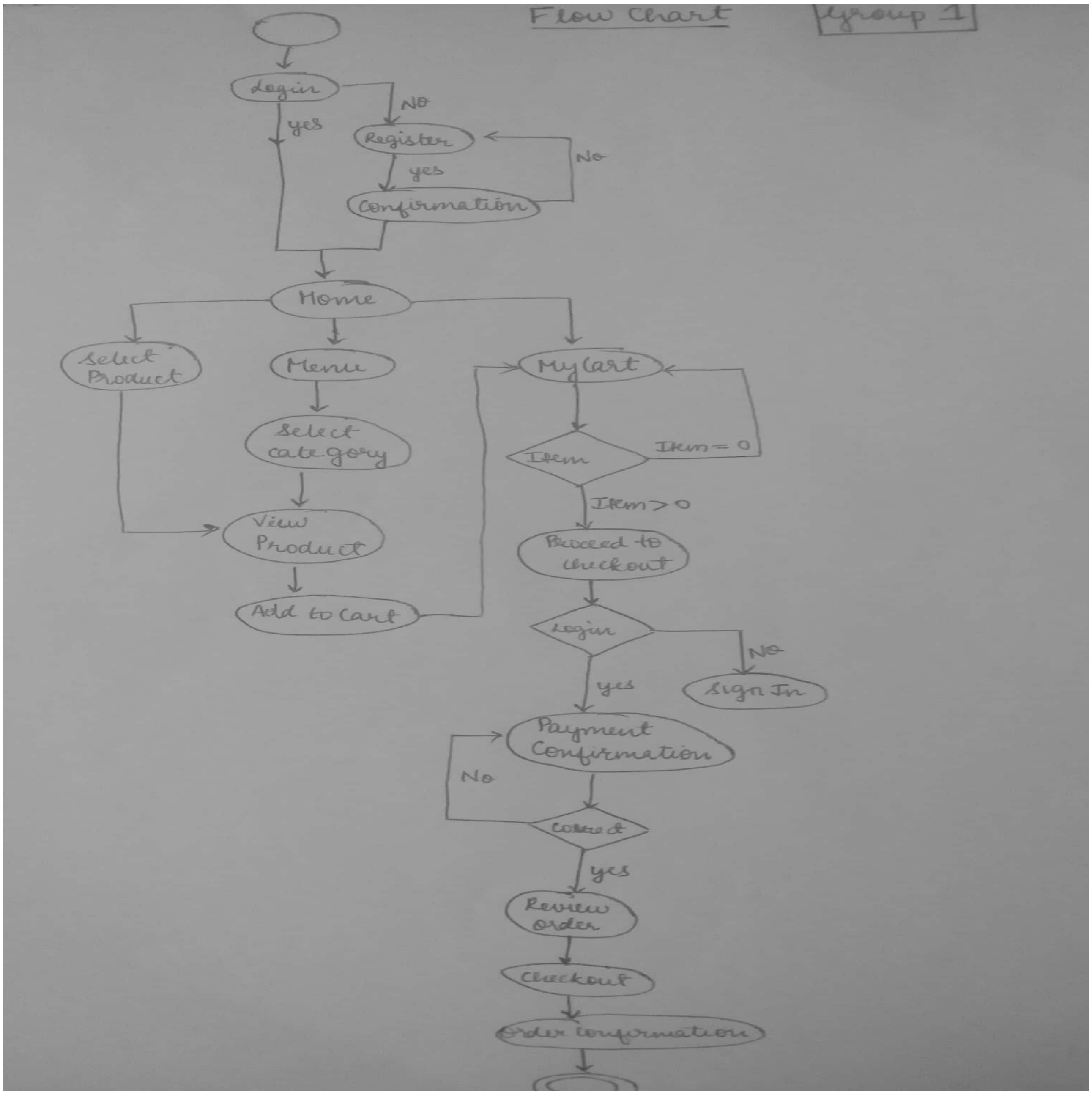
4.1.3 E-R DIAGRAM

The ER or (Entity Relational Model) is a high-level conceptual data model diagram. Entity-Relation model is based on the notion of real-world entities and the relationship between them.

ER modeling helps you to analyze data requirements systematically to produce a well-designed database. So, it is considered a best practice to complete ER modeling before implementing your database.

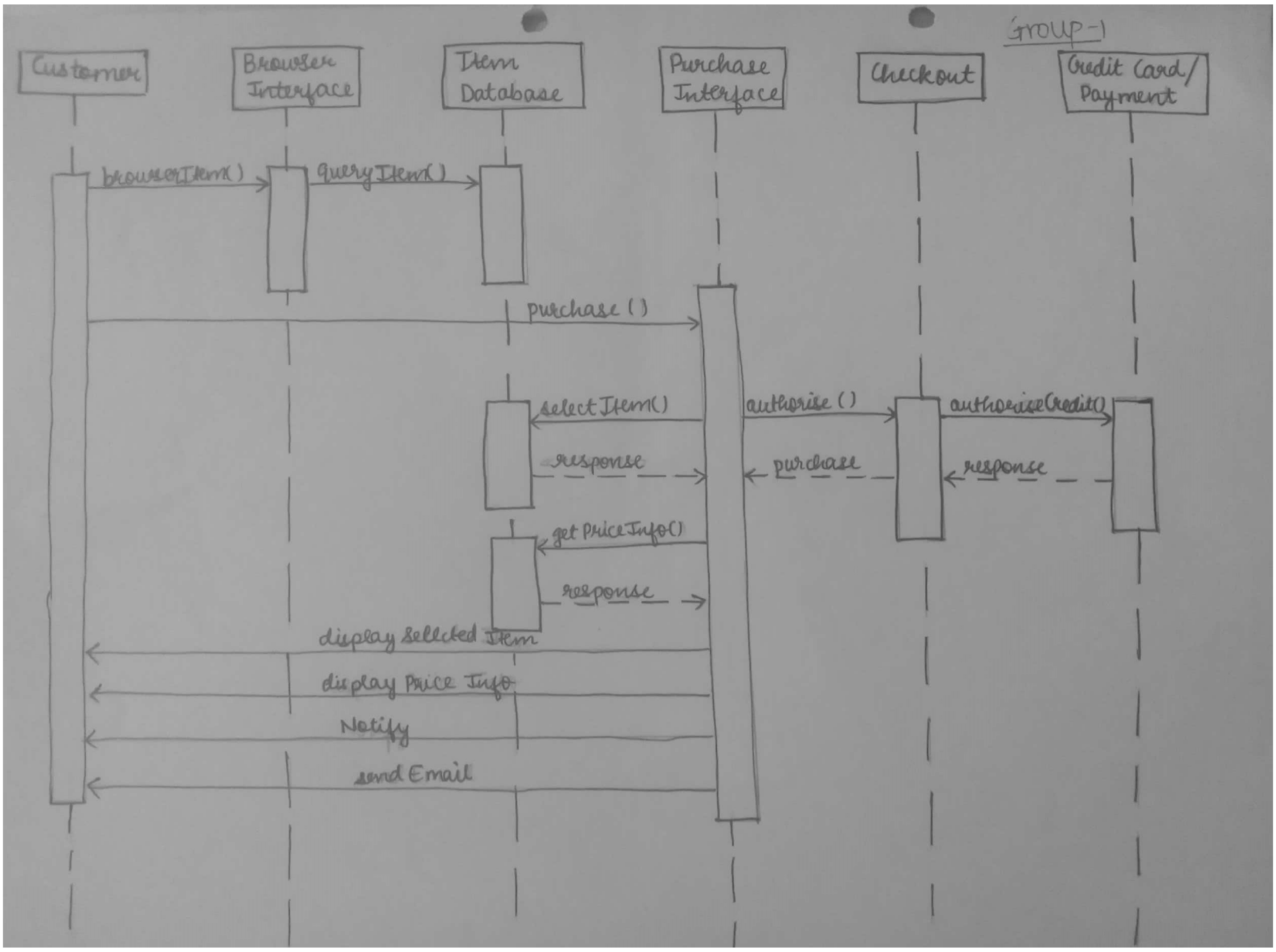

Group 1
ER Diagram
CustId
Cust Name
Customer
1
1
*
Product
Product Name
Product Details
Product_id
Has
1
Add to cart
Has
StockID
Product Stock
Stock Qty
ProdId
Cart id
Item Qty
Total Cost
Shopping Cart
1
gives
*
OrderID
Has
Order Details
Packing Cost
Packing Date
Order
Make
Payment
Payment Id
Payment Cost
Payment Date
Cart Id
Order Status
Order Id

4.1.4 FLOW CHART



4.1.5 SEQUENCE DIAGRAM

As the name suggests, sequence diagrams describe the sequence of messages and interactions that happen between actors and objects. Actors or objects can be active only when needed or when another object wants to communicate with them. All communication is represented in a chronological manner.



4.2 DESIGNING

We divided our designing phase into 2 parts-

4.2.1 SHOPPING CART APPLICATION

- **PHP** PHP is a back-end scripting language, which runs on server and it returns HTML as result which we see on our browser. It is used to store our important data in database and also retrieve it from our database.

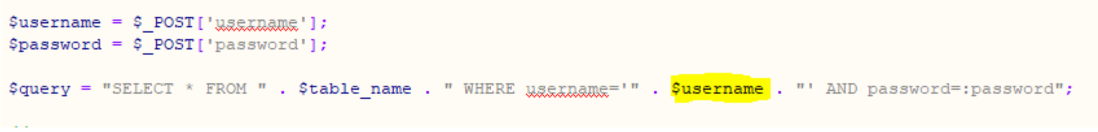
- **MySQL** SQL is the most popular language for adding, accessing and managing content in a database. It is most noted for its quick processing, proven reliability, ease and flexibility of use. MySQL is an essential part of almost every open source PHP application.

- **HTMl,CSS** Some pages were coded in HTML and styling was done using CSS.

4.2.2 INJECTING VULNERABILITIES

The following vulnerabilities were added to the application post development.

- **SQL INJECTION** SQL injection usually occurs when you ask a user for input, like their username/userid, and instead of a name/id, the user gives you an SQL statement that you will unknowingly run on your database. There are several ways to achieve SQL Injection.

  ```
  $username = $_POST['username'];
  $password = $_POST['password'];

  $query = "SELECT * FROM " . $table_name . " WHERE username='" . $username . "' AND password=:password";
  ```

  In the following snippet, we added $ username after first condition check in SQL, which comments the rest of the query, and enable user to enter any password in order to achieve login access.

5 CONCLUSION

This project helped all of us to learn various aspects of Web Development and Cyber Security. We hope this application will serve its best as an educational platform to learn various cyber threats.